

20. Колпаков В.К. Адміністративний деліктний правовий феномен: Монографія. – К.: Юрінком Інтер, 2004. – 528 с.

21. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ [Електронний ресурс] / Режим доступу: **Ошибка! Недопустимый объект гиперссылки.**

22. Кодекс Республики Беларусь об административных правонарушениях от 20 мая 2003 года // Национальный реестр правовых актов республики Беларусь от 9 июня 2003 года № 63.

23. Виконавча влада і адміністративне право / За заг. ред. В.Б. Авер'янова. – К.: Видавничий Дім "Ін-Юре", 2002. – 668 с.

24. Про внесення змін до Кримінального кодексу України щодо запровадження інституту кримінальних проступків: Проект Закону України № 10126 [Електронний ресурс] / Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb_n/webproc4_1?id=&pf3511=42706

25. Парламентарии предложили свое видение "уголовных проступков" // Юрлига [Електронний ресурс] / Режим доступу: <http://jurliga.ligazakon.ua/news/2012/3/1/58387.htm>

УДК 343.146:343.346.8:004 ■ **ПРЕДМЕТ ДОКАЗУВАННЯ У КРИМІНАЛЬНИХ
С.Ю. Гаврик ■ СПРАВАХ ПРО КОМП'ЮТЕРНІ ЗЛОЧИНИ**

В статті розкриваються проблемні питання предмету доказування у уголовних делах о компьютерных преступлениях.

Ключевые слова: *предмет доказывания, компьютерные преступления, доказательная информация.*

У статті розкриваються проблемні питання предмету доказування у кримінальних справах про комп'ютерні злочини.

Ключові слова: *предмет доказування, комп'ютерні злочини, доказова інформація.*

The problem questions of ultimate fact in criminal cases about computer offences are considered in the article.

Key words: *ultimate fact, computer offences, case-based information.*

Інформаційно-комунікаційні технології є одними з найважливіших чинників, які впливають на формування пріоритетних напрямів розвитку двадцять першого століття: надаються безпрецедентні можливості доступу до інформації, колективного її використання і взаємного обміну.

Сучасні інформаційні технології істотно змінюють не тільки структуру української економіки, але і спосіб життя, образ мислення

людей, механізми функціонування суспільних інститутів, інститутів державної влади. Наразі перше місце за значимістю впливу на такі зміни безсумнівно посідають технології комп'ютерних мереж та мереж електрозв'язку.

Водночас поряд із широкими можливостями й доступністю засобів електронно-обчислювальної техніки та електрозв'язку, особливостями технологій дистанційної обробки комп'ютерної інформації, не обмеженими адміністративними і державними кордонами, знесобленістю основної частини комп'ютерної інформації, привертає увагу правопорушників і створює передумови не лише для істотної зміни способів учинення "традиційних" злочинів, а й появи нових різновидів комп'ютерних злочинів.

Десятим Конгресом ООН щодо запобігання і контролю над злочинами, пов'язаними з використанням мережі Інтернет, Конвенцією Ради Європи про кіберзлочинність, Окінавською Хартією глобального інформаційного суспільства, декларацією Бангкока про протидію новому виду кіберзлочинців та іншими міжнародними правовими актами злочинні посягання з використанням мережі Інтернет для країн-членів ООН визнані глобальною міжнародною проблемою.

Про ступінь суспільної небезпеки злочинів указанного виду наочно свідчить той факт, що згідно з доповіддю Центру по боротьбі зі злочинами в мережі Інтернет ФБР, у США щорічно реєструється понад 336 тис. заяв від потерпілих, сукупний збиток від таких злочинів складає понад 560 млн доларів США¹.

Як проголошує Окінавська Хартія глобального інформаційного суспільства, яка прийнята державами-членами "Великої вісімки" 23 липня 2000 року, сьогодні "зусилля міжнародної спільноти, що спрямовані на розвиток глобального інформаційного суспільства, повинні супроводжуватися узгодженими діями по створенню безпечного та вільного від злочинності кіберпростору... Необхідно також знайти ефективне політичне вирішення актуальних проблем, як, наприклад, спроби несанкціонованого доступу та комп'ютерні вироуси"².

Проведений нами науковий аналіз офіційних даних ДІТ при МВС України показав, що за останні п'ять років кількість комп'ютер-

¹ 2009 Internet Crime Report [Електронний ресурс] / Internet Crime Complaint Center. - Режим доступу : http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

² Okinawa Charter on Global Information Society // G-8 Information Centre. Information System by the University of Toronto. - < <http://prod.library.utoronto.ca/g7/summit/2000okinawa/sourcedocs/it1.html> >. 14 p.

них злочинів, учинених в Україні, збільшилась майже вдвічі. При цьому, офіційна статистика не відображає реального стану загрози, яку несуть комп'ютерні злочини, що вчинені з використанням мережі Інтернет, через високий рівень їх латентності та транснаціональний характер.

Узагальнення емпіричних даних в окресленій сфері показало, що розкриття та розслідування комп'ютерних злочинів, що вчиняються з використанням мережі Інтернет, залишається досить складним завданням для більшості співробітників органів досудового розслідування та оперативних працівників. Це обумовлено, по-перше, відсутністю узагальнень матеріалів оперативної, слідчої та судової практики, методичних рекомендацій по організації розкриття та розслідування даного виду злочинів, досвіду роботи слідчих і працівників органів дізнання зі специфічними джерелами доказової інформації, що знаходиться в електронній цифровій формі у вигляді електронних повідомлень, сторінок, сайтів; по-друге, недостатнім рівнем підготовки оперативних працівників та слідчих з відповідній спеціалізації в навчальних закладах.

Однією з основних причин цього також є те, що оперативні працівники та слідчі не достатньо обізнані в предметі доказування цього виду злочину і як наслідок, оперативні працівники неналежним чином документують усі структурні елементи предмету доказування в ході оперативно-розшукової діяльності, а слідчі - неналежним чином здобувають та закріплюють доказову інформацію про них у матеріалах кримінальної справи.

Проблемні питання протидії комп'ютерній злочинності висвітлювались у працях таких українських учених, як Д. С. Азаров, А. С. Білоусов, Г. М. Бірюков, В. М. Бутузов, В. Д. Гавловський, В. О. Голубев, О. М. Джужа, Р. А. Капюжний, М. В. Карчевський, О. В. Копан, О. І. Мотлях, Ю. Ю. Орлов, Л. П. Паламарчук, Д. В. Пашнев, М. А. Погорєцький, Н. А. Розенфельд, М. В. Салтєвський, О. А. Самойленко, С. М. Сівочек, О. П. Снігер'єв, В. С. Цимбалюк, М. Я. Швець, В. П. Шеломенцев та ін.

Багато іноземних науковців також займалися дослідженням цих злочинів, зокрема Т. В. Авер'янова, В. Б. Вехов, Ю. В. Гаврилін, Р. І. Дремлюга, В. Є. Козлов, В. В. Крилов, В. О. Мещеряков, В. О. Мілашев, У. А. Мусаєва, А. Л. Осипенко, Донна Б. Паркер, Р. Повер, О. Р. Рос-сінська, Л. Н. Соловійов, К. Сегер, В. М. Черкасов, Н. Г. Шурухнов, Дж. Ховард, О. М. Яковлев та інші.

Проте предмет доказування цих злочинів, на наш погляд, є недостатньо дослідженим, що є метою цієї статті.

Враховуючи велике значення предмету доказування у кримінальному процесі й криміналістиці, необхідно мати чітке уявлення про його зміст як слідчим, так і оперативним працівникам.

Традиційно в кримінально-процесуальній науці під предметом доказування прийнято розуміти коло обставин, що підлягають дослідженню та встановленню у кримінальній справі з метою її правильного вирішення¹. Такі обставини визначаються статтями 64 і 23 КПК України.

Згідно статті 64 КПК України при провадженні досудового слідства, дізнання й судового розгляду кримінальної справи підлягають доказуванню: 1) подія злочину (час, місце, спосіб та інші обставини вчинення злочину); 2) винність обвинуваченого у вчиненні злочину і мотиви злочину; 3) обставини, що впливають на ступінь тяжкості злочину, а також обставини, що характеризують особу обвинувачуваного, пом'якшують та обтяжують покарання; 4) характер і розмір шкоди, завданої злочинцем, а також розмір витрат закладу охорони здоров'я на стаціонарне лікування потерпілого від злочинного діяння. А відповідно до статті 23 КПК орган дізнання, слідчий, прокурор зобов'язані виявляти причини й умови, які сприяли вчиненню злочину.

Окрім того, до предмету доказування входять також інші обставини: доказові факти й обставини, за допомогою котрих встановлюється об'єктивність відомостей, що містяться в тому чи іншому джерелі доказів. Під доказовими фактами слід розуміти факти, за допомогою яких встановлюються обставини, зазначені в статтях 64 і 23 КПК України, а також факти, які підлягають доказуванню у справі.

З урахуванням обмеженого обсягу статті ми зробимо спробу розкрити лише ті елементи предмету доказування комп'ютерних злочинів, які, на нашу думку, є найпроблемнішими в практиці оперативних та слідчих підрозділів.

Слід зазначити, що досягнення повноти розслідування кримінальних справ про комп'ютерні злочини можливе лише за умови встановлення всіх обставин, що входять до предмета доказування. Комп'ютерні злочини, з цієї позиції, неодноразово вивчалися вченими-правознавцями. Елементи, включені в цю категорію, є взаємопов'язаними, взаємозалежними і складають єдину систему. Труднощі з доказуванням одного елемента, поза

¹ Кримінальний процес України: Підруч. для студентів юрид. спец. вищ. закладів освіти / Ю. М. Грошевий, Т. М. Мірошніченко, Ю. В. Хоматов та ін.; За ред. Ю. М. Грошевого та В. М. Хотенця. – Харків: Право, 2000 – С. 131.

сумнівом, тягнуть за собою наслідки, що позначаються на решті елементів. Тому розглянути окремо кожен елемент предмета доказування у справах про комп'ютерні злочини можна лише умовно.

Необхідно зазначити, що окрім загальних особливостей предмета доказування за кожен комп'ютерний злочин має і свої властиві тільки йому обставини. Слідчий повинен ретельно аналізувати матеріали кримінальної справи для визначення і своєчасного доказування таких обставин, оперативний працівник повинен встановити їх оперативно-розшуковими засобами.

Конкретний комп'ютерний злочин вчинюється у властивих лише йому обставинах. Відповідно до особливостей діяння загальний предмет доказування у кримінальній справі наповнюється та індивідуалізується змістом.

Слід зазначити, що у спеціальній літературі, досліджуючи предмет доказування про комп'ютерні злочини, пропонується встановлювати такі обставини: 1. Чи був злочин. 2. Яким є об'єкт злочинного посягання (для вибору прийому виявлення під час розслідування). 3. Яким є предмет злочинного посягання. 4. Яким є спосіб вчинення злочину. 5. Місце, час (період) і обставини вчинення злочину. 6. Розмір і вид збитку, заподіяного потерпілому. 7. Хто скоїв злочин. 8. Якщо групою осіб, то якими є склад групи та роль кожного співучасника. 9. Які обставини сприяли вчиненню злочину. 10. Чи було вжито захисні заходи, засоби, способи, контрольні процедури, направлені на зниження ризику несанкціонованого доступу інформації¹.

У цьому контексті А.І. Журба зазначає, що інтерес у дослідженні предмета доказування комп'ютерних злочинів становить викладений вченими перелік обставин, що з'ясовуються під час допиту. Розглядаючи це питання, можна виявити, до якої категорії обставин, що мають значення для справи, належить той або інший елемент. Тому неможливо абсолютно точно визначити, до якого саме елемента предмета доказування належить обставина, через їх взаємопов'язаність. Автор наводить перелік зазначених елементів з такими коментарями.

1. Навички і досвід роботи з комп'ютерною технікою і конкретним програмним забезпеченням. У цілому може виступати доказовим фактом по відношенню до події злочину, обставин, що характеризують особу обвинуваченого в частині спеціальних технічних пізнань.

¹ Захарченко В.Ю., Лазуренко В.И., Олифіров А.В., Рогозин С.Н. Компьютерные преступления: их выявление и предотвращение: Учебное пособие / Под общ. ред. В.И. Лазуренко. - К.: Центр учебной литературы, 2007. - С. 116.

2. Використання на комп'ютері за місцем роботи правомірного доступу до комп'ютерної техніки і конкретних видів програмного забезпечення. Як і у вищезгаданому випадку, належить до доказового факту щодо події злочину й обставин, які характеризують особу обвинуваченого в частині спеціальних технічних пізнань.

3. Конкретні операції з комп'ютерною інформацією, які підозрюваний (обвинувачений) виконує або на своєму робочому місці, або (якщо не працює) на своєму персональному комп'ютері, або на комп'ютерах своїх знайомих. Має те саме значення, що і вказані вище два елементи.

4. Правомірний доступу до мережі Інтернет і роботи в Інтернеті. Належить до доказового факту події злочину.

5. Закріплення за підозрюваним за місцем роботи ідентифікаційних кодів і паролів для користування комп'ютерною мережею тощо. Як і попередній, цей елемент належить до доказового факту злочину.

6. Коли виник намір скоїти злочин, хто або що вплинуло на це рішення. Належить до елемента предмета доказування, пов'язаного з причинами й умовами, що сприяли вчиненню комп'ютерного злочину, і мотивом злочину.

7. Чому був вибраний саме цей об'єкт для злочинного посягання (організація, структура, де сам працював, або стороння установа, підприємство). Належить до доказового факту способу вчинення злочину і до мотиву злочину;

8. Якими є мотиви вчинення злочину. Безпосередньо належить до доказування елемента предмета доказування – мотиву злочину.

9. Яка мета переслідувалася скоєнням комп'ютерного злочину. На наш погляд, цей елемент належить до доказових фактів мотиву злочину та причин і умов, що йому сприяли¹.

На нашу думку однією з основних обставин, яку необхідно з'ясовувати під час доказування у справах, порушених за ст. 361 КК України є - доказування факту несанкціонованого втручання в роботу мережі електрозв'язку. В Законі України "Про телекомунікації" мережі електрозв'язку визначаються, як комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, провідних, оптичних чи інших електромагнітних системах між кінцевим обладнанням².

¹ Журба А.І. Особливості предмета доказування у справах про комп'ютерні злочини: Дис. ... канд. юрид. наук: 12.00.09. - Харків, 2008. - С. 59.

² Відомості Верховної Ради України. - 2004. - № 12. - Ст. 155.

При дослідженні питання предмету доказування у кримінальних злочинах важливим є розуміння що являє собою комп'ютерна інформація. Комп'ютерну інформацію як предмет злочину можна визначити таким чином: відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника і вартість.

В результаті вчинення злочину відбувається вплив злочинця на смисловий зміст комп'ютерної інформації. Розрізняють такі види впливу на зміст комп'ютерної інформації:

- знищення інформації - видалення інформації, що зберігається на будь-якому машинному носії, що створює неможливість її відновлення на ньому. Факторами, що викликають знищення інформації, можуть бути, по-перше, навмисні або з необережності дії осіб, що мали можливість впливати на цю інформацію, а, по-друге, причини програмно-технічного характеру, що пов'язані із порушеннями в роботі комп'ютерних пристроїв та систем;

- модифікація інформації - це внесення змін в програми та будь-яку іншу інформацію, що зберігається на матеріальному носії окрім її легальної модифікації. Діючим законодавством дозволені такі види легальної модифікації програм та іншої інформації особами, що правомірно володіють цією інформацією, як модифікація у вигляді виправлення очевидних помилок, внесення змін в програми, бази даних для їх функціонування на технічних засобах користувача та часткова декомпіляція програми для досягнення здатності до взаємодії з іншими програмами;

- копіювання інформації - це перенесення інформації на інший, відокремлений від ЕОМ носій із збереженням незмінною первинної інформації, відтворення інформації в будь-якій матеріальній формі рукописно, шляхом фотографування тексту з екрану дисплея, а також зняття інформації шляхом перехоплення випромінень ЕОМ тощо.

Середовищем існування комп'ютерної інформації є файлова система, що становить сукупність інформаційних одиниць - файлів, спеціальних службових таблиць, завантажувальних записів, таблиць розташування файлів і кластерів. Файли мають фіксовану структуру і характеристики, що підтримуються операційною системою, встановлення яких має криміналістичне значення.

Під час доказування необхідно керуватися тим, що доводити слід зовнішній прояв злочинної поведінки, який містить більш знач-

ну кількість інформації, необхідної для правильної кримінально-правової кваліфікації. Дослідження цих ознак є чи не найголовнішим етапом доказування події злочину, передбаченого ст. 361 КК України. Правильне та ретельне дослідження ознак об'єктивної сторони складу злочину сприяє точній правовій оцінці суспільно-небезпечного діяння та є запорукою законності в процесі розслідування кримінальної справи.

Кримінально-процесуальному пізнанню й доказуванню у справах про злочин, передбачений ст. 361 КК України має бути піддане несанкціоноване втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку. Ця діяльність пов'язується із доведенням трьох конститутивних ознак – суспільно небезпечного діяння, суспільно небезпечних наслідків та причинно-наслідкового зв'язку між суспільно-небезпечним діянням та суспільно-небезпечними наслідками.

У юридичній літературі з кримінального процесу існують різні підходи й щодо визначення черговості пізнання обставин вчинення злочину. Так А.І. Журба вважає, що під час розслідування кримінальної справи, порушеної за ознаками вчинення злочину, передбаченого ч.1 ст. 361 КК України, а саме здійснення несанкціонованого втручання в роботу комп'ютера, що спричинило модернізацію інформації, – відповідно до п.1 ст. 64 КПК України встановленню підлягає: місце, час, спосіб здійснення несанкціонованого втручання і результат, що настав у вигляді зміни інформації¹. Вчений пропонує дослідження події комп'ютерних злочинів і доказування у справах цієї категорії розпочинати з дослідження саме місця вчинення злочину.

На нашу думку така пропозиція є недостатньо обґрунтованою. Процес доказування факту вчинення злочину логічно розпочинати з встановлення вчинення певного діяння, про що свідчать не лише місце, а й час, спосіб й інші обставини вчинення злочину (п. 1 ч. 1 ст. 64 КПК України). Далі, послідовно необхідно встановлювати й доказувати протиправність та суспільну небезпечність діяння. Це підтверджують і результати проведеного анкетування: на питання "Які ознаки об'єктивної сторони складу злочину підлягають першочерговому встановленню і доказуванню в справах про злочин, передбачений ст. 361 КК України?", переважна більшість слідчих (94%) та співробітників оперативних підрозділів МВС України (85%) відповіли, що це – суспільно-небезпечне діяння.

¹ Журба А.І. Вказана праця. – С. 106.

Підсумовуючи викладене, зазначимо, що у кримінальних справах про комп'ютерні злочини підлягають доказуванню:

1. Подія комп'ютерного злочину (час вчинення і настання наслідків, місце, спосіб та інші обставини вчинення комп'ютерного злочину і суспільно небезпечних наслідків. (Особливо у разі дистанційного способу вчинення. Більш детально це питання ми розглянемо в підрозділі, присвяченому події комп'ютерного злочину).

2. Вчинення обвинуваченим комп'ютерного злочину, мотиви, цілі.

3. Обставини, що впливають на ступінь тяжкості комп'ютерного злочину, а також обставини, що характеризують особу обвинуваченого, пом'якшують або обтяжують покарання. У цьому елементі необхідним є доказування обставин як тих, що безпосередньо впливають на покарання (ставлення до праці, суспільства тощо), так і тих, що виражаються в технічних пізнаннях, пов'язаних із можливістю особи скоїти злочин, які, крім того, можна віднести до непрямих доказів.

4. Характер і розмір шкоди, заподіяної комп'ютерним злочиним. Необхідно довести зміну інформації та її належність до матеріальних цінностей (електронні гроші, акції) або її безпосередню цінність (дані, що містять комерційну таємницю тощо).

5. Причини й умови, що сприяли вчиненню комп'ютерного злочину. Цей елемент необхідно доводити як із технічної позиції (слабка безпека інформації, системи комп'ютерного захисту у потерпілого та ін.), так і із соціальної (неправильне виховання, особливості кола спілкування обвинуваченого та ін.).

Кожен із зазначених нами елементів предмету доказування у кримінальних справах про комп'ютерні злочини може бути окремим предметом наукового дослідження.

УДК 342.951

М.О. Керезора

**МАТЕРІАЛЬНО-ПРАВОВІ ПІДСТАВИ
ЗАСТОСУВАННЯ ПОПЕРЕДЖЕННЯ ЗА ВЧИНЕННЯ
АДМІНІСТРАТИВНИХ ПРАВОПОРУШЕНЬ**

У статті проаналізовані матеріально-правові підстави застосування попередження та аналогічних за змістом заходів впливу у зв'язку з вчиненням адміністративних правопорушень. Виділені нормативно-правові підстави і особливості застосування попередження до юридичних осіб.

Ключові слова: *відповідальність, правопорушення, стягнення, попередження, заходи впливу.*